Chapter 1: Introduction to Strong Authentication at Fermilab

In 2001 Fermilab implemented new methods for users to access the computers at the FNAL site. The purpose of this introduction is to summarize the method and explain what it means for you as Fermilab computer users, system administrators, and software developers.

1.1 Computing on the World Wide Web

The landscape of the computing environment has changed dramatically from the days when the Internet was primarily the domain of the academic research community. The same explosive growth in computing hardware, network connectivity, and capable software that has enabled HEP to tackle the daunting computing challenges of our field have led to a tremendous increase in the pool of participants on the Internet. There has been increasing "urbanization" of the Internet. This means, among other things, that the previous methods of access control are insufficient for today's needs.

1.2 Strong Authentication

The new access methods involve a concept known as "strong authentication".

> Strong authentication is a system of verifying the identities of networked users, clients and servers without transmitting passwords over the network. It does not require that the network be protected. Both parties in a connection must demonstrate knowledge of some "secret" to establish their identities.

The strong authentication service implemented at Fermilab is the Kerberos Network Authentication Service V5. Kerberos (throughout the manual, "Kerberos" refers to Kerberos V5) is a network authentication protocol designed to serve as a trusted third-party authentication service. It verifies the identity of a user or a network service (users and services are collectively

called *principals*) on an unprotected network using conventional cryptography in the form of a shared secret key. In addition to establishing identity (authentication), it supports encrypted network connections, thereby providing confidentiality.

The "heart" of a Kerberos installation is the Key Distribution Center (KDC). All the computers associated with a KDC make up what's called a *strengthened realm*. At Fermilab, there are two strengthened realms: there is one for UNIX machines called FNAL.GOV, and for Windows 2000 systems there is FERMI.WIN.FNAL.GOV. The KDC's main functions include:

- Maintaining a database of users and services within its realm.
- Authenticating users by way of exchanging tickets between clients and services in the strengthened realm.

1.3 Why has Fermilab implemented strong authentication?

There have been several computer security breaches at Fermilab and other DOE facilities. Our funding agencies has required Fermilab to demonstrate that it has implemented a computer security system that exercises tight control over who uses the lab's computers and network.

In response, Fermilab has issued revisions to its Computing Policy that detail responsibilities and requirements for accessing computing resources at Fermilab. The Computing Policy is provided online at `http://www.fnal.gov/cd/main/cpolicy.pdf`. We provide the relevant information from the policy in more readable language in Chapter 2: *Fermilab Computing Policy Issues*.

This manual seeks to explain the implementation of Strong Authentication at Fermilab. Where there appear to be conflicts, the Policy prevails.

1.4 What do you need to know and do ?

Virtually all machines at Fermilab require Kerberos authentication for network access. You will need to be able to satisfy that authentication requirement in order to gain access. How you satisfy it depends on the role you play in your use of computers (e.g., user or administrator), on the OS you use, and on whether you connect from your machine over the network to other machines or not.

If you bring a machine from your university to FNAL, the machine must be Kerberized if you wish to participate in the strengthened realm. We highly recommend that you participate, as it makes your access to other FNAL machines much simpler.

For those of you at a university or other off-site location, you may include your machine in the FNAL Kerberos realm as well. Off-site machines have different requirements for doing so.

1.4.1 General User

As a general UNIX or Windows user, you should expect that the maintainer of your computer has provided the basic tools and installation necessary to configure the machine as a member of Fermilab's strengthened realm.

Your responsibilites are listed below:

General User Responsibilities	Where to find Information
(Recommended) Understand the broad outlines of Fermilab's Strong Authentication policy.	Read the entire Part I: *Getting Started*, especially Chapter 2: *Fermilab Computing Policy Issues*.
Obtain a Kerberos principal (an identifier for the realm, akin to a login name) and a Kerberos password.	See section 3.1.2 *Requesting a Principal*, or go straight to the online form at `http://computing.fnal.gov/cd/forms/actreq_form.html`.
Obtain a CRYPTOCard if necessary, learn how to use it, and care for it properly.	You can find out what a CRYPTOCard is used for and determine whether you need one by reading section 4.4 *Connecting from a NonKerberized Machine: Portal Mode*. Care and use of CRYPTOCards are described in Chapter 5: *Using your CRYPTOCard*.
Change your initial Kerberos password to an acceptable one of your choosing within 30 days of receipt.	See sections 3.2.2 *Choosing a Kerberos Password*, and 3.3 *Changing your Kerberos Password*.
Learn how to obtain your login credentials.	How to do this depends on whether you're logging in to a Kerberized machine at the console or over the network, on what software you're using, and on other factors.)
Learn how to use your login credentials without exposing them to theft.	See section(s) of Chapter 4: *Accessing Kerberized Machines (Fermilab-Supported Methods)* appropriate to your operating system(s), and Chapter 11: *Encrypted vs. Unencrypted Connections*.

General User Responsibilities	Where to find Information

And last but not least: Treat your Kerberos password as a sacred object!!

- Your Kerberos password must be known only to you.
- Make sure that you do not write it down anywhere that someone could find it.
- Do not put it in a file (encrypted or not).
- As a usual practice, type it only at the console of a system on which you authenticate.
- Only on very rare occasions, when you have no other choice, may you pass it over a network connection. The connection MUST BE ENCRYPTED. Verify that ALL connections in the chain are encrypted.
- Choose a character string different from your Kerberos password for all other passwords and other objects. (The one exception: your passwords for the FNAL.GOV and FERMI.WIN.FNAL.GOV realms may be the same.)
- If you mistakenly type your Kerberos password over an unencrypted channel, please change your password immediately!

Windows Desktop Users

Windows desktops and resources at Fermilab are for the most part in the Windows 2000 domain. The W2K domain structure supports Kerberos authentication. For information on this, see *Windows 2000 at Fermilab* at `http://computing.fnal.gov/cd/windows/w2kdoc/`.

1.4.2 System Administrator

As a system administrator (including those who administer their own machines), you need to do and understand everything the general user does, and in addition, you must understand how to setup the Kerberos tools and how to properly configure the machine for the strengthened realm. For users of the Computing Division's UPS/UPD environment, much of this has been automated. Also a number of system vendors are providing Kerberos as a standard option within their OS installation. You may use whichever tools you prefer as long as the result complies with Fermilab policy. The obligation is on you, the adminstrator, to understand your own configuration well enough to ensure compliance. The chapters in the Administrator part of the manual provide detailed instructions on many common circumstances at the lab.

1.4.3 Developer

You as an application or system developer need to understand the principles of strong authentication, and the Fermilab Computing Policy in detail. It is your responsibility to design systems and software that enhance the security of Fermilab's computing systems and to improve our ability to withstand the onslaught of attackers who would misuse our resources.

1.5 What advantages does Kerberos provide?

One big advantage is that you have *one* id, known as your Kerberos principal, and *one* password that can be used anywhere at the lab (actually two principals: name@FNAL.GOV and name@FERMI.WIN.FNAL.GOV). This simplifies life considerably. You still need authorization to use machines to which you log in (an account or an entry in an access control list), but there are no passwords that need to be locally maintained anymore.

Once you are authenticated on a system, you can move from one strengthened machine to another without having to type your password again.

And, most importantly, the computers *are more secure* from abuse by outsiders.

For more information, see Appendix A: *Implementation Details of Strong Authentication at Fermilab* and Appendix B: *About the Kerberos Network Authentication Service V5*.

1.6 What advantages does Kerberos have over other possible solutions?

In Kerberos V5, the password-checking (authentication) happens in one place, and the end systems need not store any information which can be used to try to guess a password. Further, Kerberos allows a single point of disabling an unauthorized or wayward user on all systems in the strengthened realm. This feature satisfies one of Fermilab's obligations to the DOE.

In ssh, as in standard UNIX, each end system has to store information sufficient to check the password, which is therefore also sufficient to try to guess the password. If the RSA authentication method is used, the RSA keys can give access to various accounts, and there's no way to know with certainty

who possesses which keys. In the event of a compromise of a private key, there's no mechanism for locating every host on which the corresponding public key appears.

1.7 How does Kerberos work?

Kerberos authentication operates by the exchange of tickets that allow access to all services by the user in the strengthened realm. This first sample scenario shows how it works when a user connects over the network from a Kerberized UNIX desktop to a remote Kerberized UNIX host:

1) User first logs in directly (not over the network) to a Kerberized desktop computer that is in the FNAL.GOV realm.

2) User requests authentication for the FNAL.GOV realm, and must enter his or her Kerberos password.

3) Behind the scenes: Kerberos software installed on the desktop is used to derive a key from the password. This key is used to encrypt the exchanges between the local machine and the (remote) KDC in order to achieve authentication. The password is not transmitted between the two machines.

4) When authentication is complete, user gets a "ticket" (also called a "credential") from the KDC.

5) The user can now connect over the network to other Kerberized hosts without entering his Kerberos password again. Without entering ANY password, in fact! Kerberos negotiates the authentication for each login using the ticket, all behind the scenes.

This second scenario shows how it works when the user's UNIX desktop is not Kerberized; this is where CRYPTOCards come in (see Chapter 5).

If the local desktop computer does not run Kerberos software and is not part of the FNAL.GOV realm, then the user can't authenticate locally on this computer. The user can work on the desktop with no problem, but in order to connect to remote Kerberized UNIX hosts, he or she must authenticate to FNAL.GOV first. Here's how it works:

1) The user logs into desktop computer normally, and enters his or her standard password.

2) From the desktop machine, the user opens a connection to a remote Kerberized host machine.

3) Kerberized machines in the FNAL.GOV realm are configured to require entry of a single-use password whenever they receive a login request coming from an unKerberized computer over the network. (The password gets transmitted over the network, and it could get intercepted. That's why it must be single-use only.)

How do you get a single-use password that Kerberos will recognize and honor? The FNAL.GOV realm at Fermilab is setup to use CRYPTOCards to provide these single-use passwords.

1.8 How do you obtain a Kerberos Principal?

To request a principal, use the online form at http://computing.fnal.gov/cd/forms/acctreq_form.html. But first, read more about principals in Chapter 3: *Kerberos Principals and Passwords*.

After you get a principal, you'll need to change your initial Kerberos password that comes with it. If your experiment or group doesn't have a Kerberized machine set up yet, or if you don't have an encrypted connection to a Kerberized machine, log into any of the FNALU machines to change your password and to get acquainted with Kerberos.